UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/764,233	01/23/2004	Neeraj Gaur	2003P04916US01	8462

7590 06/20/2006

Siemens Corporation
Attn: Elsa Keller, Legal Administrator
Intellectual Property Department
170 Wood Avenue South
Iselin, NJ 08830

EXAMINER	
CAI, WAYNE HUU	

ART UNIT	PAPER NUMBER
2617	

DATE MAILED: 06/20/2006

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	Application No.	Applicant(s)	
	10/764,233	GAUR, NEERAJ	
	Examiner	Art Unit	
	Wayne Cai	2617	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *09 May 2006*.

2a)☒ This action is **FINAL**. 2b)☐ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1,3-5 and 7-20* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1,3-5 and 7-20* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____ .
5) ☐ Notice of Informal Patent Application (PTO-152)
6) ☐ Other: _____.

DETAILED ACTION

The Art Unit location of your application in the USPTO has changed. To aid in correlating any papers for this application, all further correspondence regarding this application should be directed to Art Unit 2617.

Claims 1, 3-5, and 7-20 are pending.

Response to Arguments

1. Applicant's arguments filed May 12, 2006 have been fully considered but they are not persuasive.

The applicant has amended claim 1 in order to overcome previous rejection under 35 U.S.C. 112, first paragraph. Hence, the rejection is now withdrawn.

In response to applicant's argument that the present application discloses the benefit of transferring the digital rights information associated with a first mobile device to the second mobile device through maintaining decryption information in a removable data card allowing a user to upgrade to a newer model of the mobile device without incurring costs to re-acquire the rights, the fact that applicant has recognized another advantage which would flow naturally from following the suggestion of the prior art cannot be the basis for patentability when the differences would otherwise be obvious. See *Ex parte Obiaya*, 227 USPQ 58, 60 (Bd. Pat. App. & Inter. 1985).

In response to applicant's arguments against the references individually, one cannot show nonobviousness by attacking references individually where the rejections are based on combinations of references. See *In re Keller*, 642 F.2d 413, 208

USPQ 871 (CCPA 1981); *In re Merck & Co.*, 800 F.2d 1091, 231 USPQ 375 (Fed. Cir. 1986).

The Examiner firstly notes to the Applicant that both Bremer and Tarpenning teach or suggest the method and apparatus for distributing, and managing protected content. More specifically, Tarpenning teaches or suggests transferring decryption information from the first device to the second device (see fig. 5 of Tarpenning and its descriptions). In addition, Bermer teaches or suggests that both encrypted content and decryption information would be able to store/handle using a subscriber identify module card (SIM). For example, some device certificates could be stored on the SIM card as well as private key storage, and operations (see paragraphs 0056 of Bremer).

Therefore, the Examiner disagrees with the Applicant's statement at the last paragraph on page 7 of Remarks, "Bremer and Tarpenning fail to disclose the system and method for maintaining media objects from a first mobile device to a second mobile device employing a removable card. Content protected by digital rights management mechanisms may be transferred to a second device and may only be decrypted with the specific removable data card employed with the first mobile device." because the fact that Bremer clearly teaches at paragraphs 0039-0056 that the encryption and decryption keys needed to be transmitted and verified between devices and/or servers in order for user to gain access to the encrypted content. The international mobile equipment identity (IMEI) number, mobile station integrated service digital network number (MSISDN) is used to identify the subscriber. The digital rights management (DRM) on the other hand contains the secure creation and storage of the private DRM

key. The authentication process is known in the art, and unless the provided information is matched, then subscriber could have access to the encrypted content. The Examiner further notes that this information is stored in the memory (e.g., memory of the mobile phone, SIM card, etc.) Bremer even explicitly discloses that the encrypted or decrypted information could be stored on the SIM as well (see paragraph 0056). Hence, it is clear to one skilled in the art that without a specific SIM card or removable data card that stores specific decryption information, then the encrypted content would not be able to decrypt and provide the content to subscriber.

For example, a room has valuable information, and being locked. The key is provided to open only that particular room. When different key is inserted into the lock hole, one would not be able to open/unlock it because the lock would not recognize or match the inserted key with the lock. It is the same as the mobile device containing encrypted content. The decryption key is provided to decrypt the encrypted content, and it is stored in a specific removable data card. Therefore, when different removable data card is inserted into the same mobile device or even different mobile device, then the encrypted content would not be able to recognize or find a match with the provided decryption key. Hence, subscriber would not have an access to the encrypted content.

In addition, the Applicant requests additional documents in supporting the obviousness statement the Office made previously. In response to the request, the Examiner hereby submits Oshima (US 6,463,300 B1) as another reference where Oshima teaches detecting whether or not the mounted integrated circuit (IC) card is same as an IC card mounted when the mobile communication terminal has previously

accessed a network as a previous IC card. Oshima specifically teaches at column 6, lines 28-47 that the memory section 25 has a secret number storing section 251 for storing a secret number registered in the mobile station 10 itself. **The controller 21 judges whether or not the inserted SIM card 26 is the same as the previously inserted SIM card 26 by comparing the part of various data storing the SIM data storing section 252 and the obtained data.**

Therefore, it is obvious to one skilled in the art that even without concerning about the digital rights content for a moment, the prior art clearly teaches that the mobile device has capability to detect when different removable data card (i.e., SIM card) is inserted, and only the authorized, pre-stored information are matched, then subscriber has access to the mobile device. Hence, when the decrypted is generated and stored on the specific removable data card, and different removable data card is inserted into the same mobile device. One could not be able to get the encrypted content for two reasons as set forth above. Firstly, the encrypted content requires the decrypted information in order to open the encrypted content. Secondly, since the decrypted is stored in a specific removable data content, but it is now being removed and inserted with a different removable data card. Therefore, the encrypted content would not detect the desired decryption information; in turn, subscriber cannot access to the encrypted content.

Once again, the fact that inserting a different removable data card into the mobile device and expecting to get access to encrypted content is impossible, and it is clearly obvious to one skilled in the art.

Claim Rejections - 35 USC § 103

2. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

3. Claims 1, 3-5, 7-9 are rejected under 35 U.S.C. 103(a) as being unpatentable over Bremer (US 2003/0174838 A1)

Regarding claim 1, Bremer discloses a method for providing authorized access of copy-protected content to an authorized user of a mobile device, comprising:

- receiving content (paragraph 0030, i.e., the second terminal 14 receives content that is forwarded by the first terminal 12);
- encrypting said content, said encrypted content being stored in memory of a mobile device (paragraph 0030 teaches the first terminal 12 encrypts the protected content and inherently the protected content is stored in a memory of the terminal);
- generating decryption information for said encrypted content; said decryption information being stored within specific removable data card (see paragraph 0056) within said mobile device (paragraphs 0033-0034, and 0046);
- providing said unencrypted content upon said mobile device when said specific removable data card containing decryption information for said encrypted content is detected within said mobile device (paragraph 0035).

It is obvious to one skilled in the art that when a different removable data card is inserted, then the content would not be able to decrypt the encrypted content because the removable data card does not have the same decryption information. For further details, refer to explanations set forth in arguments section above.

Regarding claim 3, Bremer discloses the method as described in claim 1 as described above. Bremer also discloses wherein decryption information (i.e., a private key of the second terminal 14) of said encrypted content is stored in a secure location of said specific removable data card.

Regarding claim 4, Bremer discloses the method as described in claim 1 as described above. Bremer further discloses said specific removable data card being at least one of a subscriber identity module card and a removable user interface module card (paragraph 0056).

Regarding claim 5, Bremer discloses a method of providing copy-protected content to a mobile device, comprising:

- transferring content to a mobile device (i.e., the first terminal 12 forwards content to the second terminal 14)), said content being in an encrypted format (paragraph 0030);
- transferring digital rights information (i.e., includes a device certificate of the terminal 12) for decrypting the content to said mobile device, said digital rights information being stored within a specific removable data card within said mobile device (paragraph 0034);

- wherein the content in said encrypted format is able to be decrypted upon the detection of the specific removable data card containing said digital rights information (paragraph 0049).

The Examiner also rejects limitation, "the content being prevented from decryption when a different removable data card is inserted within said mobile device" at least for the same reasons set forth in claim 1 and explanations set forth in argument section.

Regarding claim 7, Bremer discloses the method as described in claim 5 as described above. Bremer also discloses wherein said digital rights information (i.e., the device certificate) for decrypting content is stored in a secure location of said specific removable data card (paragraphs 0034, and 0056).

Regarding claims 8, and 9, Bremer discloses the method as described in claim 5 as described above. Bremer further discloses wherein the mobile device is a mobile telephone (see fig. 1), and wherein said removable data card is at least one of a subscriber identity module card and a removable user interface module card (paragraph 0056).

4. Claims 10-20 are rejected under 35 U.S.C. 103(a) as being unpatentable over Bremer (US 2003/0174838 A1) in view of Tarpenning et al. (hereinafter "Tarpenning", US 6,513,117 B2).

Regarding claim 10, Bremer discloses the method as described in claim 5 as described above, except for wherein said content transferring step comprises

downloading said content over-the-air or downloading said content via a computer coupled to said mobile device.

In a similar endeavor, Tarpenning discloses a certificate handling for digital rights management system. Tarpenning further discloses wherein said content transferring step comprises downloading said content over-the-air or downloading said content via a computer coupled to said mobile device (col. 4, lines 15-31).

It would have been obvious to one of ordinary skill in the art at the time the invention was made to include the step of downloading said content so that the information could be transferred from one device to anther device.

Regarding claims 11, and 16, Bremer discloses a method, in a system including a first mobile device and a second mobile device, for maintaining copy-protected content, comprising:

- encrypting content locally within said first mobile device (paragraph 0046);
- transferring encrypted content stored within said first mobile device to said second mobile device (fig. 1, elements 12 & 14).

Bremer, fails to disclose:

- transferring a specific removable data card including digital rights information associated with said first mobile device to a receptacle of said second mobile device;
- decrypting said encrypted content transferred from said first mobile device on said second mobile device when said specific removable data card including

said digital rights information has been detected within said second mobile device.

In a similar endeavor, Tarpenning discloses a certificate handling for digital rights management system. Tarpenning further discloses:

- transferring digital rights information associated with said first mobile device to a receptacle of said second mobile device (fig. 5, element 1045 and its descriptions);
- decrypting said encrypted content transferred from said first mobile device on said second mobile device when said digital rights information has been detected within said second mobile device (col. 8, lines 45-58).

The Examiner also notes that even though neither Bremer nor Tarpenning specifically discloses transferring a specific removable data card. However, Bremer does teach that some device certificates could be stored on the SIM card (i.e., a specific removable data card) as well as private key storage and operations (see Bremer, paragraph 0056). On the other hand, Tarpenning teaches transferring digital rights information from the first device to the second device. The Examiner further notes that this digital rights information must be stored in a secure place of a memory. Therefore, it would have been obvious to one skilled in the art to modify both Bremer, and Tarpenning's invention to arrive at the present invention by storing the digital rights information on the removable data card.

It would have been obvious to one of ordinary skill in the art at the time the invention was made to include the steps of transferring the digital rights information

associated with the first mobile device to the second mobile device because it adds a flexibility for user to upgrade to a newer model of the mobile device without incurring costs to re-acquire the rights. In addition, the owner of the protected information still gets protections at the same time.

Regarding claims 12, and 17, Bremer and Tarpenning disclose the method as described in claims 11, and 16 as described above. Tarpenning further discloses preventing decryption of said content when the User Certificate is not installed, or detected within said second mobile device (col. 8, lines 45-58).

Regarding claims 13, and 18, Bremer and Tarpenning disclose the method as described in claims 11, and 16 as described above. Neither Bremer nor Tarpening specifically teaches wherein transferring encrypted content includes removing a removable media disk storing encrypted content from said first mobile device and inserting the removable media disk into the second mobile device.

However, it is obvious to one skilled in the art that the claim feature is not novel because it is known that the content could be stored on the removable data card (i.e., SIM card). Therefore, by removing the removable data card that is stored an encrypted content from one mobile device to another device is not novel.

Regarding claims 14-15, and 19-20, Bremer and Tarpenning both disclose the method as described in claims 11, and 16 as described above. Bremer also discloses wherein the mobile device is a mobile telephone, a mobile handset, a personal digital assistant (PDA), or pager (fig. 1), and wherein said specific removable data card is at

least one of a subscriber identity module card and a removable user interface module card (paragraph 0056).

Conclusion

5. **THIS ACTION IS MADE FINAL.** Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the mailing date of this final action.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Wayne Cai whose telephone number is (571) 272-7798. The examiner can normally be reached on Monday-Friday; 9:00-6:00; alternating Friday off.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Duc Nguyen can be reached on (571) 272-7503. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

Wayne Cai
Examiner
Art Unit 2617

ELISEO RAMOS-FELICIANO
PRIMARY EXAMINER